



CYBERSTALKING SURVIVORS' RIGHTS IN THE DIGITAL AGE: BRIDGING THE GAP BETWEEN CRIMINAL LAW AND ONLINE REALITIES

**Goswami Apeksha
Sukhdevpuri**

Research Scholar, Department of Law, Gokul Global University, Siddhpur,
Gujarat

ABSTRACT

Cyberstalking was now a formidable form of Internet abuse, facilitated by the omnipresence of connectivity, anonymity, and cross-platform communication. Laws, which traditionally focused on physical bullying, had struggled to respond to stalking that existed in technology. This essay examined how current criminal law paradigms are inconsistent with the reality of internet victimization and the victim experience. The United Kingdom and India were matched to compare statutory evidence, judicial interpretation, and capacity of institutions to address cyberstalking. The research design was a doctrinal and secondary qualitative thematic approach, analyzing legislation, case law, and literature. The findings indicated that both jurisdictions had formally acknowledged cyberstalking; however, there were inherent deficiencies in conceptual and theoretical clarity, evidentiary practice, and protection of victims. Procedural delays, difficulties with digital evidence, and a deficiency of trauma-informed support undermined access to justice. The paper emphasised how survivor-centered change in the law, improved governance of digital evidence, improved platform accountability, and improved cross-border cooperation are needed to bridge the divide between criminal law and online realities.

KEYWORDS : Cyberstalking, Digital Harm, Criminal Law, Online Harassment, Comparative Law

1. INTRODUCTION

The consequences of cyberstalking are psychological, emotional, and reputational harm that directly affects the autonomy, privacy, and dignity of victims. Despite this pressure, the rights of survivors do not properly become a part of the criminal justice response. The existing legal processes tend to be more evidence-based and criminal-oriented instead of survivor protection and trauma-informed practice-oriented. The absence of a practical application to assist survivors in online contexts and the substantial expression of injury can be considered in Survivor Safeguarding in Protection against Harassment Act 1997 and in Malicious Communications Act 1988.

Criminal law evolved in relation to bodily being, proximity, and apparent repetition. Cyberstalking contravenes these assumptions because of the anonymity, cross-platform, and automated communication. Even with the adoption of new legislation, such as the Online Safety Act of 2023 in the United Kingdom and the Indian Penal Code of Section 354D, the definition and protocol are often rigid, which serves as a barrier to the effective safety of people. The judicial review often relies on the analogy to offline behavior, restricting the doctrinal remaking of online realities.

2. Research Aim, Objectives, and Scope

The primary aim of the study is to examine the adequacy of criminal law frameworks in protecting cyberstalking survivors within digital environments.

The objectives are:

- To analyses how cyberstalking is conceptualized within existing criminal law frameworks.
- To examine procedural and evidentiary barriers affecting survivor access to justice.
- To assess institutional capacity in addressing technology-enabled stalking.
- To propose survivor-centered legal and policy reforms.

3. Conceptual and Theoretical Foundations of Cyberstalking

In general, cyberstalking can be characterized as the online actions that are unwanted and unwelcome and cause distress, fear, or personal disruption. The authors indicate that cyberstalking is a continuation of different types of harassment into new digital formats where repetitions and insistence are no longer determined by physical proximity, but

by constant connectivity to the Internet (Jurasz and Barker, 2021). This perspective highlights the value of digital communication devices in assisting in long-term tracking and connection, which can be realized anywhere or any time.

On the other hand, Hijazi et al. (2024) expect that one of the cross-platform characteristics of cyberstalking is that it is becoming increasingly difficult to define the concept consistently in court since behaviour is manifested simultaneously on social media networks, messaging applications, and email services. Anonymity also complicates this definition, as it allows the criminals to avoid detection and accountability.

Physical stalking or physical contact has traditionally characterized stalking, but, lawwise, cyberstalking is mingled and discouraged. This has also been attempted by the courts, as in *R v Debnath* [2005] EWCA Crim 3472, where online harassment was governed by the Protection from Harassment Act 1997.

Cyberstalking is not an issue of inconvenience but the realm of complete online victimization. Ailwood et al. (2023) acknowledge that legal responses fail to listen to the voice of survivors in most instances and that efficiency of procedures is valued more than lived experience. This criticism portrays the untold psychological and emotional harm, including anxiety, fear, and powerlessness, of the criminal justice processes. On the contrary, Knipschild et al. (2025) indicate that the idea of digital harm should be put through the multidisciplinary understanding of reputational damage and long-term trauma as harmful as the physical one.

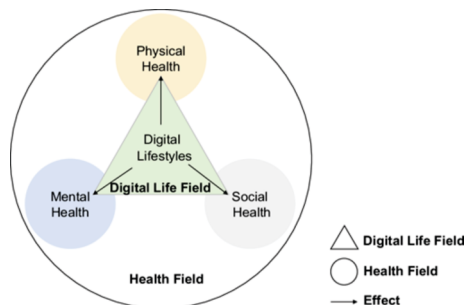
The problem of cyberstalking on the international level is incredibly problematic due to the absence of uniformity in the definitions and the absence of unity in legislation. According to Marcos (2023), the absence of single legal principles undermines the consistency of international law, particularly in the case of cross-border digital damages. Quite the contrary, Laajasalo et al. (2023) assume that definitional inconsistency is not only legal but also operational, and it conditions how the harm is perceived and dealt with by institutions. This kind of fragmentation leads to unfair inter-jurisdictional protection and enforcement.

4. Literature Gap

The literature provides a conceptual breakdown on the topic

of definitional ambiguity, digital harm, and gendered vulnerability in cyberstalking. However, the crevassing of survivor-compensated views to criminal law doctrine is commensurably despicable. The current body of literature has a tendency to concentrate on legal designs or power of survivors in single instances, and very little is known about how legal practice can turn statutory protection into lived justice. More so, little attention is paid to how far cross-platform behavior and anonymity undermine the evidentiary standards in the field. This kind of division demands a system that consolidates the doctrinal analysis, institutional capacity, and the right of the survivors to comparative legal systems.

5. Theoretical Framework



Digital Harm Theory informed the paper, conceptualizing harm as a result of structural design and affordances of digital environments, and not individual behaviour. The Digital Harm Theory emphasizes the power of minute details in the construction of platform functionality, presence in algorithms, and continuous connectivity to increase victim exposure and mental impact. This theory can be applied to cyberstalking to know why the current criminal law theories are unsuitable in addressing cumulative harm over the internet.

6. Research Methodology

The research method used to study cyberstalking and its legal effects is mainly qualitative, with some use of doctrinal analysis. This means the focus is on looking at current laws, court rulings, academic writings, and policy documents related to cybercrime. The study mainly uses secondary data, such as research papers, legal publications, government reports, and court cases. Thematic analysis is used to spot common themes in how cyberstalking is defined, handled in court, and experienced by victims. The study also compares different legal systems, especially between India and places like the United Kingdom. This helps in learning about good practices around the world and finding out where domestic laws might be lacking. The approach focuses on careful interpretation rather than using data from experiments or surveys, and aims to give a thorough understanding of the legal and conceptual aspects of cyberstalking.

7. Criminal Law Frameworks Addressing Cyberstalking

Criminal laws dealing with cyberstalking have changed to keep up with the challenges brought by digital communication. In India, cyberstalking is mainly covered under Section 354D of the Indian Penal Code, which makes it a crime to stalk someone, including using electronic ways to monitor or contact them. The Information Technology Act, 2000 also has rules about online harassment, stealing identities, and using data improperly. However, even with these laws, it's hard to enforce them because of things like online anonymity, issues with legal authority across borders, and the technical nature of digital crimes. On the other hand, places like the United Kingdom have more complete laws, such as the Protection from Harassment Act 1997 and the Online Safety Act 2023. These laws put more responsibility on digital companies and offer more help to victims. They also focus on stopping harassment before it happens, holding platforms accountable, and supporting those affected. While there are

laws in place, how well they work depends on how well they are carried out, the technology available, and working together internationally to deal with the fact that cyberstalking can happen anywhere online.

8. CONCLUSION

The authors had come to the conclusion that cyberstalking became a ubiquitous form of online abuse that could not be addressed by the existing criminal law system. Comparative analysis of the United Kingdom and India has revealed that even though the laws on the protection against harassment, such as Protection from Harassment Act 1997, Malicious Communications Act 1988, Online Safety Act 2023, and Section 354D of Indian Penal Code and information technology Act 2000 formally recognize cyberstalking, the reality was unbalanced. The act was lax regarding the construction of the law by the courts: jurisprudence could accommodate *R v Debnath* [2005] EWCA Crim 3472, but the concepts must be anchored in offline law to restrict intelligibility of the doctrine over the internet.

These findings were also added to the debate on cyberstalking and victim rights by demonstrating how legalization did not result in adequate protection. Procedural inefficiencies, evidence barriers, and institutional capacity still impede the process of ensuring that all survivors get justice. The review further found that the experiences of the survivors were habitually excluded from the criminal processes that culminated in the re-experience and lack of access to litigation. The interdependence between the doctrinal analysis and the view of the survivor was used to appreciate the detachment between official law and lived justice in a better manner.

9. REFERENCES

- Radoniewicz, Filip. *Cybercrime and the Law: An Analysis of Legal Governance in Europe*. Taylor & Francis, 2025.
- Kumar, Ashutosh, and Adv Priya Ranjan. "Prevailing Cyber Security Law." *Supremo Amicus Journal* PIF 6 (2022).
- DeGloma, Thomas. Anonymous: The performance of hidden identities. University of Chicago Press, 2023.
- Bhushan, Mayank, and Aatif Jamshed. *Cybercrime and Digital Security: Understanding threats, attacks, and defenses in the connected world* (English Edition). BPB Publications, 2025.
- McLachlan, Katherine J. *Trauma-informed criminal justice: Towards a more compassionate criminal justice system*. Switzerland: Palgrave Macmillan, 2024.
- Journals**
- Wilson, Channele, Lorraine Sheridan, and David Garratt-Reed. "What is cyberstalking? A review of measurements." *Journal of Interpersonal Violence* 37, no. 11-12 (2022): NP9763-NP9783.
- Samanta, Prasad. "Cyberbullying and Online Aggression: Patterns, Predictors, and Prevention." *Research Journal in Psychology and Behavioral Studies* 2, no. 1 (2025): 25-37.
- Rackley, Erika, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, and Anastasia Powell. "Seeking justice and redress for victim-survivors of image-based sexual abuse." *Feminist Legal Studies* 29, no. 3 (2021): 293-322.
- Manoj, Daniel, Ranjit Immanuel James, Senthil Kumaran, Gerard Pradeep Devnath, Benji Tom Varughese, Antony L. Arakkal, and Latif Rajesh Johnson. "Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation." *Child Protection and Practice* 4 (2025): 100088.
- Ailwood, Sarah, Rachel Loney-Howes, Nan Seuffert, and Cassandra Sharp. "Beyond women's voices: Towards a victim-survivor-centred theory of listening in law reform on violence against women." *Feminist Legal Studies* 31, no. 2 (2023): 217-241.
- Knipschild, Rik, Milou Covers, and Iva AE Bicanic. "From digital harm to recovery: a multidisciplinary framework for First Aid after Online Sexual Abuse." *European Journal of Psychotraumatology* 16, no. 1 (2025): 2465083.
- Lajjasalo, Taina, Laura Elizabeth Cowley, Gabriel Otterman, Diogo Lamela, Leonor Bettencourt Rodrigues, Andreas Jud, Alison Kemp et al. "Current issues and challenges in the definition and operationalization of child maltreatment: A scoping review." *Child Abuse & Neglect* 140 (2023): 106187.
- Berkowitz, H  loise, and Michael Grothe-Hammer. "From a clash of social orders to a loss of decidability in meta-organizations tackling grand challenges: The case of Japan leaving the International Whaling Commission." In *Organizing for societal grand challenges*, vol. 79, pp. 115-138. Emerald Publishing Limited, 2022.
- Lavorgna, Anita, Pamela Ugwuodike, and Yadira Sanchez-Benitez. "Harms of digital capital: social harm analysis of online public resistance and information pollution." *Justice, Power and Resistance* 5, no. 3 (2022): 249-269.